J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust Management Systems for Wireless Sensor Networks: Best practices", *Computer Communications*, vol. 33, pp. 0140-3664, 2010.
http://doi.org/10.1016/j.comcom.2010.02.006
NICS Lab. Publications: https://www.nics.uma.es/publications

Trust Management Systems for Wireless Sensor Networks: Best Practices

Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago

Department of Computer Science, University of Malaga, Malaga 29071 Spain

Abstract

Wireless Sensor Networks (WSN) have been proven a useful technology for perceiving information about the physical world and as a consequence has been used in many applications such as measurement of temperature, radiation, flow of liquids, etc. The nature of this kind of technology, and also their vulnerabilities to attacks make the security tools required for them to be considered in a special way. The decision making in a WSN is essential for carrying out certain tasks as it aids sensors establish collaborations. In order to assist this process, trust management systems could play a relevant role. In this paper we list the *best practices* that we consider are essential for developing a good trust management system for WSN and make an analysis of the state of the art related to these practices.

Key words: Wireless Sensor Networks, Trust Management, Best Practices

1. Introduction

Computer systems are not able to perceive the physical information of the real world by themselves. It is possible to use sensor hardware to convert a physical property (e.g. temperature, radiation) into a digital signal. However, it would be interesting to have a component, either application-specific or off-the-shelf, which provides the functionality of a *sensory system* to any kind of computer system. That is the task of Wireless Sensor Networks (WSN). The primary elements of a WSN, the sensor nodes, are constrained

Email address: {jlm,roman,isaac,mcgago}@lcc.uma.es (Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago)

devices capable of sensing and processing the information of the environment. Besides, they can use a wireless channel to collaborate among themselves. Finally, they are able to send the information to powerful devices known as base stations, which act as front-ends of the WSN, providing data to any human or non-human user (e.g. a RTU in a SCADA system [1]). The benefits of using WSN technology are numerous: it is easy to deploy and not expensive mainly due to the use of a wireless interface (cf. [16] for an industrial example), and it is able to run unattended and survive in its deployment area for long periods of time (e.g. a year or more [12]).

While self-sufficiency is considered to be one of the major features of WSN, this property does not come into existence automatically: it needs to be enforced. The elements and protocols of a WSN must be prepared to cope with variable conditions, faulty nodes and malicious entities. One mechanism that can be used to support the decision making processes of the network is a Trust Management System. It aids the members of WSN (trustors) to deal with uncertainty about the future actions of other participants (trustees). By evaluating and storing the reputation ("What is generally said or believed about a person or the character or standing of a thing") of other members, it is possible to calculate how much those members can be trusted ("the firm belief in the reliability or truth or strength of an entity") to perform a particular task.

The importance of trust management systems in WSN has been acknowledged by the research community, and there exist many approaches that pursue the creation of a functional and lightweight system. However, many of these approaches do not take into account some specific features of WSN that can influence over their construction and functionality.

It is the purpose of this paper to derive certain trust management *best practices* from the specific features of WSN, and to analyze the compliance of the actual state of the art on trust management systems with those *best practices*. As an output of this analysis, we can identify those aspects that need to be further developed in present and future systems.

The structure of this paper is as follows. In section 2 we introduce the general characteristics of WSN, provide an overview of trust management systems, and show the importance of trust management systems for WSN. Section 3.1 provides an analysis of the actual state of the art and Section 4 discusses how the systems studied in the previous section fulfill certain *best practices*, which should be taken into account on the development of any trust system. Finally, we present our conclusions on Section 5.

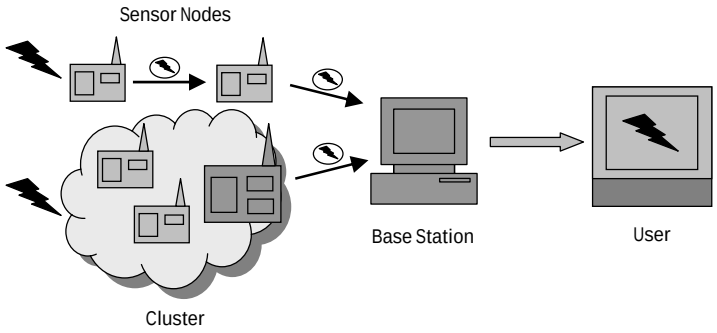

Figure 1: An Overview of the Architecture of WSN

2. Sensor Networks and the Importance of Trust

2.1. Elements and Features of Sensor Networks

While modern research on sensor networks started on the late seventies [6], this paradigm acquired an identity of its own at the beginning of the twenty-first century [21]. Present-day sensor networks can be considered as *living beings*, usually *born* (configured) in a controlled environment, where all its nodes are *cells* that work selflessly towards a common goal. Such nodes can work autonomously and are able to perform various tasks. The overall architecture of a WSN is highly dependent on its intended functionality. Another relevant feature of these networks is that no human user directly controls the nodes: they are usually accessed through the base station. Finally, WSN are usually long-lived, and the sensor nodes may have limited mobility [32].

From a technological perspective, as shown in Figure 1, a WSN is mainly composed of two types of devices: sensor nodes and base stations. The sensor nodes, also known as motes or simply nodes, are small and constrained devices equipped with hardware sensors, microcontrollers, transceivers and batteries. Hardware sensors are used to sense the physical features of the environment (e.g. temperature, humidity, radiation, vibration). Microcontrollers are highly constrained in both computational power and memory, but thanks to them nodes are capable of processing information on their own. Wireless transceivers enable nodes to collaborate towards a common goal, such as routing the information to a base station. Finally, most nodes are battery-powered thus, they can survive in their deployment field for more than a year if their internal operations are optimized [12].

The base station is a more powerful device that behaves as a *front-end* between the services provided by the sensor nodes and the users of the network. While it would seem that WSN are highly dependent on the existence of this base station, the architecture of the network is not centralized. The nodes operate in a decentralized fashion, managing themselves without accessing the base station. In fact, there are some specific networks, known as *unattended sensor networks*, where the base station is only available at certain moments in time. Still, the base station usually plays an important role on the overall behaviour of WSN. Normally, a base station collects all the information coming from the sensor nodes and stores it for later use. Also, it may issue control orders to the sensor nodes in order to change their behaviour.

The network architecture of a WSN can be organized in a completely distributed way (flat configuration), but it can also implement levels of hierarchy (hierarchical configurations). In flat configurations all the nodes contribute in the decision-making process and participate in internal protocols such as routing. Conversely, in hierarchical configurations the network is divided into clusters or group of nodes. Inside a cluster all organizational decisions, like data aggregation, are made by a single entity called cluster head. It should be noticed that it is also possible to have a combination of the two previous configurations into the same network; for instance, to avoid situations where the *spinal cord* of the network - the cluster heads - fails and the information must be routed to the base station.

Regarding the services offered by wireless sensor networks they can be classified into four major categories: monitoring, alerting, provisioning of information *on-demand* and actuating. Due to the computational capabilities of the sensor nodes, it is also possible to re-program the network during its lifetime, or even use it as a distributed computing platform under specific circumstances.

- **Monitoring.** Sensor nodes can continuously monitor certain features of their surroundings (e.g. measuring the ambient noise level) and timely send such information to the base station.

- **Alerting.** Sensor nodes can check whether certain physical circumstances (e.g. a fire) are occurring, alerting the users of the system when an alarm is triggered.

- **Information *on-demand*.** The network can be queried about the

actual levels of a certain feature, providing information whenever the user needs it.

- **Actuating.** Sensor nodes can be able to change the behaviour of an external system (e.g. an irrigation system) according to the actual state of the context (e.g. humidity of the soil).

There have been many experimental applications (from environmental monitoring to smart environments) created by the research community that take advantage of the previously shown WSN services [9]. For example, sensor nodes are very useful in precision agriculture [35], where they can improve the quality of the crops through actively managed irrigation. Moreover, a specific application that has attracted the attention of the industrial community is nuclear power plant monitoring [4], where sensor nodes can provide real-time information of the radiation levels of both workers and physical structures of a nuclear power plant. We believe that potential markets for WSN are likely to be increased drastically in the next coming years mainly due to recent developments in the field. This prediction is based on the rapid adoption of WSN in the areas mentioned above during the last few years.

2.2. Security and Trust

The emerging importance of sensor networks could be hindered by their inherent security problems. This technology is tightly associated to the physical world. Thus, the nodes are as accessible as the event they monitor. The wireless channel used in the communications can also be accessed by anyone. Also, the nodes are highly constrained in terms of computational power, memory, communication bandwidth and battery power. Consequently, any malicious adversary could launch a certain set of attacks that could render the network partially or totally useless.

In order to solve the security problems present in WSN, a set of security primitives that could improve the robustness and the reliability of the network should be included. For example, cryptographic primitives are needed in order to create secure communication channels; and the security credentials used by those primitives must be distributed using key management systems. Besides, additional services, such as self-healing and trust management services, should exist. They can help to protect the *core* protocols of the network: aggregation, time synchronization and routing. Finally, other aspects such as distributed computing, secure location, secure mobile base station location need to be protected, if included inside a sensor network.

Trust management can help improving the security of WSN. For example, for the routing process, sensor nodes might need to know which other nodes to trust for forwarding a packet. For sensing purposes a node might need to trust other neighbouring nodes for checking anomalous measurements. Other examples of trust in sensor networks include data disclosure decisions and key exchange. However, as sensor nodes are usually constrained devices, the trust management systems must be lightweight enough to provide a good performance without hindering the functionality of the system. Moreover, due to the distributed nature of those networks, trust management systems for them are susceptible to attacks. According to [34] some of the most common attacks to a trust management system for WSN are:

- **Bad mouthing attack.** When taking recommendations into account in a trust management system we take the risk of receiving dishonest recommendations. Some nodes may also try to bad mouth an honest node that has reported them as dishonest previously. This causes a fear for retaliation which might result in a recommendation that does not reflect the real opinion of the recommender. See Figure 2.A. Note that arrows represent recommendations and black nodes represent the dishonest nodes.

- **On-Off attack.** If bad behaviour can be compensated with good behaviour, dishonest nodes can take advantage of it and behave well and badly alternatively. Thus, they can remain trusted while behaving badly. See Figure 2.B.

- **Selective behaviour attack.** The trust system may accept recommendations only from certain relevant nodes or from all the neighbouring nodes. If a node behaves well from the point of view of most of their neighbours, it can still behave badly with respect to the rest of the nodes. This way, the average recommendation will remain positive, while it can cause damage to certain nodes. See Figure 2.C.

- **Sybil attack and newcomer attack.** If a node can create, emulate or impersonate different nodes in the network it can manipulate the recommendations and promote itself as a respected node. These attacks are also related to the white-washer attack, where a node can throw away its bad reputation by creating a new identity. See Figure 2.D.

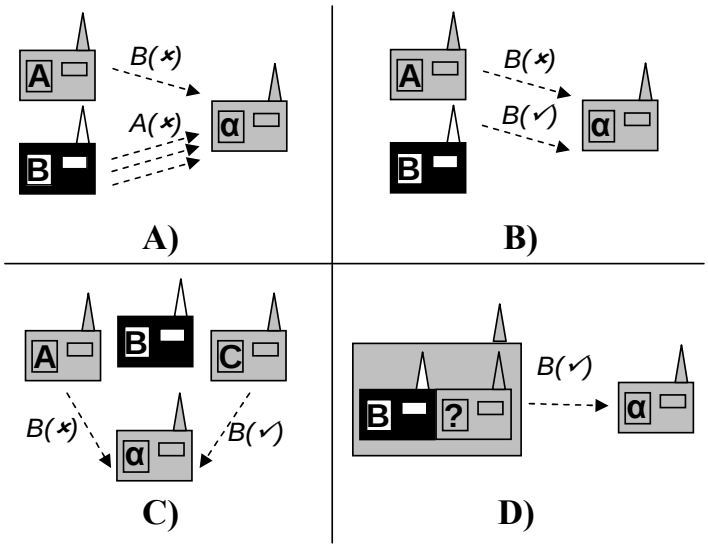

Figure 2: Representation of Different Attacks in WSN Trust Systems

2.3. Suitability of Trust

Given the previously mentioned attacks that can affect the functionality of a WSN, it may be argued that adopting a trust management system for WSN does not bring enough advantages. Nevertheless, as we will see in this section, trust is an important tool that can solve one of the intrinsic problems of WSN: the problem of uncertainty in collaboration. Besides, trust established between nodes can be used for other purposes beyond collaboration. Moreover, once the possible attacks against a trust management system are known, it should be possible to create more robust systems.

Regardless of these benefits, it is also necessary to point out that trust management is not one of the foundational elements that enables the creation of a fully functional wireless sensor network. For example, existing standards and specifications for industrial sensor networks, such as WirelessHART [15], do not define trust (on the behaviour of other nodes) as one of their building blocks. Nevertheless, as discussed in this section, trust management is a suitable component for the security architecture of a sensor network, as it can solve some problems and provide many interesting advantages if applied correctly.

In order to explain the suitability of trust for sensor networks, we will start with the concept of collaboration. All the members of a WSN (sensor

nodes and base stations) need to collaborate in order to provide the services of the network. Examples of these collaboration processes are sensing and routing. All sensor nodes use their sensing hardware in order to obtain physical information from the environment. As many sensors can be deployed within a small area, it is possible to aggregate the information provided by those sensors if the user of the network is only interested in a general overview of the environment. Besides, every node behaves as a router, forwarding the physical information to the base station through other nodes. Nodes can choose whether to prioritize speed over energy by sending the information either through the fastest link or through the nodes that have spent less energy.

For assuring a successful collaboration, a node should be able to discover which nodes are more likely of accomplishing a certain task. If a node knows in advance how the different elements of the network will react in any situation, then it will be able to make a flawless decision. However, in a WSN the outcome of a certain situation cannot be clearly established or assured. That is, we need to take uncertainty into account.

Uncertainty is originated basically from two sources: information asymmetry (a partner does not have all the information it needs about others) and opportunism (transacting partners have different goals). For sensor networks where no node behaves maliciously opportunism is not a problem: all the elements of the network work towards a common goal and have neither reason nor the will to behave egoistically. However, information asymmetry might be a problem, as a sensor node can malfunction or the state of the environment (e.g. the wireless channel) can change. Besides, if there are subverted nodes acting maliciously inside a WSN, both information asymmetry and opportunism have to be considered. Therefore, a node cannot know in advance how a transacting partner is going to behave.

Trust management systems provide a satisfactory solution to the problem of uncertainty. While it is not possible to know the future in an accurate way, the past actions of the nodes are reflected in the reputation and trust values. If a node behaved satisfactorily in the past for performing a certain task, it is assumed that it will be reliable in the future for performing the same task. As a result, a node could start a cooperation process with the most reliable nodes. The underlying Trust Management System of WSNs will help on detecting faulty and malicious nodes

The primary purpose of using trust in WSN is closely linked to self-sufficiency: a Wireless Sensor Network must be able to configure itself not

only during the normal operation of the network, but also in under extraordinary events. By knowing the reputation of nodes in their neighbourhood and their actual behaviour, it is possible for the nodes to choose a suitable course of action when making operational decisions (knowing which is the best partner for starting a collaboration) or in extreme situations (e.g. nodes malfunctioning).

Self-configuration is not the only benefit of trust: a trust management system can also assist and/or take advantage of other security protocols and mechanisms (e.g. hardware protection, IDS, key management, privacy). Regarding hardware protection, existing code obfuscation and code attestation schemes can be easily integrated into a trust management system as tools for testing the integrity of an untrusted node. Besides, complex services such as secure location and intrusion detection systems can benefit from the existence of a trust management system, either by using the output of the system as an assistant in their decision-making process, or by providing useful trust inputs that could be useful for any other service.

The existence of a trust management system can also assist the activities of Key Management Systems (KMS) and privacy-related mechanisms. A node can use the trust measurements to revoke the keys of an untrusted entity. Nodes can also use trust to select which neighbour is going to collaborate in the distribution of a pair-wise key [28]. Finally, sensor networks can use trust as a tool to control the disclosure of information: the trust assigned to each data requestor can be used in order to determine if the data or only a sample of it will be disclosed, or if the request will be rejected [13].

3. Extracting Trust Best Practices from the State of the Art

3.1. Overview on Existing Trust Management Systems

The field of trust management systems for WSN is becoming of interest within the research community in the recent years although it is still in an early state. A lot of effort has been done in the area of trust management systems for P2P or Ad Hoc networks (see [31, 26] for a survey on these systems). However, these systems do not fit all the requirements and features required by WSN. As mentioned, this research area is becoming very active and several surveys have been produced [31, 3, 14]. Still, many of the solutions are designed with the purpose of solving very specific problems and most of them do not deal with all the features that a trust management sys-

tem for WSN should provide. In the following, we will provide an overview of the state of the art in Trust Management for WSN.

Due to the distributed nature of WSN, most of the existing trust management systems (such as [38]) propose a distributed trust model which enables a subset of the nodes to evaluate the behaviour of neighbouring nodes and make decisions about them. The trust values are usually obtained taking into consideration different parameters such as personal reference (values obtained by first-hand interaction with the nodes, also known as direct trust) and reference (information obtained from non-personal interaction, also known as indirect trust). Newer trust management systems consider the existence of additional parameters, such as dispositional trust (the amount of risk the node is ready to take) [24]. As one of the main tasks of these systems is to model the behaviour of a node, the existence of more parameters should be considered as a benefit.

The way of modelling and computing trust and reputation is also very important. The models can be very simple, where one can use discrete values such as 0 for *untrusted* or 1 for *trusted*, for example, or even include intermediate states such as *medium trusted* by using a value in between 0 and 1. Simple approaches such as using a linear function are also widely spread in the area of trust for WSN. This is the case of [24], where the trust value is represented as a continuous variable over a specific range, (-1, +1). Using these linear functions, it is possible to specify a threshold according to the risk of the operation. Consequently, a certain trust value can be labelled as *untrusted* or *trusted* in a dynamic way.

Regarding the computation of trust, some trust management systems do not take reputation into account, and directly obtain the trust values as a weighted combination of direct trust and indirect trust. For example, in [30] the nodes collect information about other nodes by taking into account the context and their experience records. This information is then computed by using the mean and the variance in order to create a confidence interval. As the significance of an event may be different between observing nodes the confidence interval is created around a weighted mean. The authors consider a formula for creating the confidence interval based on the variance and the calculation of different weights. Other trust management systems [20] also consider other external factors that may affect trust such as how trust gradually weakens between devices that no longer collaborate.

As reputation provides some interesting benefits to trust management systems (e.g. better management of aspects such as aging), some of them

propose reputation-based frameworks where nodes maintain reputation for other nodes and use it in order to evaluate their trustworthiness. For example, in [18] reputation is represented by a Bayesian formulation, more specifically, a beta reputation system. Another probabilistic function is used in [2] where the monitor nodes acquire information about other nodes by direct observation and store it as a beta distribution parameters tuple. Other systems use the Bayes theorem for combining different sources of information. For instance, [27] introduces a Gaussian reputation system for mixing second-hand information from neighbouring nodes with directly observed information.

Another factor that must be taken into account in any trust management system is the location of the trust entities, that is, the nodes that can check whether a certain trustee can be trusted or not. In most cases, any node in the network will be able to act as a trust entity since all of them have to cooperate towards a common goal. The Base Station (BS) can also take the role of a trust entity, as it has a global view of the state of the network. Nevertheless, few trust management systems consider the BS as a trust entity. One example is RDAT [29], which proposes a model that evaluates trustworthiness of nodes based on characteristics such as sensing, routing and aggregation. It makes use of a Beta reputation system, and all the calculations and routing are done through the BS.

Other approach that can be used in order to distribute the trust entities is to use clusters. In fact, some sensor networks group their nodes into clusters for various reasons (e.g. better energy management or use of more powerful nodes to execute complex tasks). The manager of the cluster is known as cluster head, and it can be in charge of analysing the trust index and making event decisions. This is the case of TIBFIT [23], a protocol that aims to detect and mask arbitrary node failures in an event-driven WSN where the nodes are organized into clusters. Still, not all cluster-based systems place the trust entity only in the cluster head. An example is [33], where the authors consider a lightweight group-based trust management scheme that combines centralized and distributed schemes. Also, in [37] the cluster head is not in charge of disseminating information about other nodes but the nodes themselves are in charge of gathering information and disseminating it among their neighbour clusters using a simple trust model based on the reputation of the nodes.

Another way of distributing trust entities is by considering agent-based systems. ATRM [5] is an agent-based trust and reputation management

scheme where the nodes are not able to manage and compute their own trust and reputation method. Thus, the ATRM model requires that every node locally holds a mobile node in charge of managing trust and reputation on its hosting-node. The system is based on a clustered WSN with backbone where its core is a mobile agent system. In [19] only a few nodes (or agent nodes) are in charge of performing operations such as storing and calculating reputation values of their neighbours. Then, the resulting values are distributed to other nodes using a broadcast method.

As previously mentioned, some trust management systems are designed for solving very specific problems. This is the case of [36], where the problem of aggregation has been tackled by using clusters whose cluster heads acts as a gateway between the cluster and the base station (BS). Moreover, some efforts have been don in order to solve the problem of selecting the most trusted cluster head [8, 7] using the underlying trust management system of the WSN.

Finally, some other trust management systems are worth to be mentioned as they introduce new approaches for managing trust and reputation. For example, a very unusual way to measure trust is adopted in [11] where *Entropy* (i.e. measure of the uncertainty associated with a random variable) is used in order to determine the relative trustworthiness between two nodes. This relative trustworthiness can be compared to the overall trustworthiness of the network in order to detect attacks. Trust is simply a numerical summary of the recommendations, which are based on the reported experiences of earlier interactions.

3.2. Introducing Trust Best Practices

The typical features of WSN (cf. Section 2.1) influence on how a trust management system should be designed in order to work in a WSN setting. This influence can be explicitly stated by defining a set of *best practices* that any trust management system for WSN should take into account. As a consequence of our analysis of various literature reviews [22, 10] and surveys [31] we have identified a set of these *best practices* which are enumerated below.

I. **Considering Trust and Reputation.** A trust management system for WSN should calculate *trust* and *reputation* separately. Reputation values are referred to the behaviour of the different entities in the network. These values could be used as inputs in order to determine trust values. By not calculating the trust directly from the behaviour of a

node, it is possible to better handle aspects such as the evolution of the node, aging, etc. For example, a malicious and untrusted node that suddenly becomes good should not be immediately trusted.

II. **Trust and the Base Station.** The base station should be able to participate in the trust management process. A base station can use the information produced by the sensor network in order to observe and analyze the behaviour of its nodes, storing their reputation values and making global trust decisions. In fact, the information asymmetry of the base station is smaller than that of the sensor nodes. The base station has a global point of view of the state of the network, whereas sensor nodes can only manage to observe their immediate surroundings. Besides, even if a base station makes no decision about the trust level of its nodes, it should receive trust information from the nodes for logging, monitoring and maintenance purposes. Note that a base station can also issue orders and send queries to the nodes of the network (e.g. do not trust node X or provide information about node Y) by using secure mechanisms such as public key cryptography.

III. **First-Hand Information Gathering.** The events that occur during the lifetime of a WSN can be used as inputs for a trust management system, as they model the behaviour of a certain sensor node. Some events are related to the specific protocols that implement the particular application provided by the network. Others are more generic and exist regardless of the underlying protocols and services: hardware-related errors, deviations from the sensor readings, issues in the communication layer, remaining energy, etc. All this wide range of first-hand information should be taken into consideration when developing a trust management system: different sources of trust information will produce a more robust trust system.

IV. **Second-Hand Information Gathering.** Reputation information about other nodes should be distributed, as this is an extremely important property of trust management systems. Neglecting the use of such second-hand information may result in decisions that are not fully consistent with the actual state of the network. Besides, since a sensor node is an entity with limited intelligence, it can detect a deviation from its own behaviour and warn other nodes about this particular situation (similar to the *apoptosis* process of living cells). Nevertheless,

due to the possible existence of subverted nodes trying to launch a bad mouthing attack, a trust entity for sensor networks must be able to integrate honest reports in spite of the existence of false and contradictory reports.

V. **Initial Values.** Any trust management system must initialize their trust and reputation values before the deployment of the network. In fact, at the beginning of the lifetime of the WSN all its nodes must have a good reputation and be equally trusted. The reason is simple: before deployment, sensor nodes are programmed with similar tasks and services in a controlled environment by the network manager and their hardware is supposed to be tested for failures. Besides, at the very beginning of the deployment state, any malicious adversary had neither the time nor the chance to influence or subvert a node. It should be noted, however, that new nodes that appear during the lifetime of the network should not be completely trusted, as they might be nodes subverted by an adversary (e.g. launching a white-washer attack).

VI. **Granularity.** While calculating the reputation of a node and its trust measurements, it is essential to take into account the granularity of the trust management system. The reputation of a certain node is built according to its behaviour and the events it triggers. However, the actions of the nodes are not reduced to the execution of one task. For example, a node can route information to the base station and read the physical measurements of its environment using the sensors, amongst others. A node needs to maintain separate opinions about the existing actions of other nodes. Thus, it needs a different set of reputation values. Besides, different trust values should also exist: a specific trust value (e.g. routing) cannot be used in most cases to deduce what the peer could do in a different task (e.g. sensing).

VII. **Updating and Aging.** The internal state of the trust management system must be updated with information received during the lifetime of the network. In addition, new information must not overwrite existing information, as trust is built over time and the node must remember the previous state of the network. Regarding aging, during the updating process trust entities should use aging mechanisms as a way to incorporate new information in a smooth way. Nevertheless, different events should not have the same impact on the reputation of a node, since

some events are a clear indication of malicious or erroneous activities. In addition, the evolution of the reputation and trust values is also an important factor that cannot be ignored. A trust entity must remember if a node achieved high *bad* ratings in the past. These countermeasures could prevent certain *on-off* attacks.

VIII. **Risk and Importance.** Two factors that should influence on the calculation of the trust values for a node are the risk of the interaction between the trustor and the trustee and the importance of the reputation value in that specific interaction. Risk and importance also should influence when selecting a threshold. That is, when a certain trust value labels a trustee as *trusted* or *untrusted* for a certain operation.

4. Analyzing Trust Management Systems through the Best Practices

4.1. Best Practices and the State of the Art

In this section we will discuss whether each of the principles introduced in section 3.2 are met by each of the proposals presented in Section 3.1. The approaches that do not fulfil any of the aforementioned practices are not cited.

Table 1 summarizes the analysis where the level of fulfilment is expressed by ×(for not achieved), - (for neutral) and ✓(for achieved).

	[37]	[29]	[24]	[20]	[7]	[2]	[19]	[11]	[27]	[25]	[30]	[5]
I	×	✓	×	×	✓	✓	✓	×	✓	✓	×	✓
II	-	-	×	×	×	×	×	×	×	×	×	×
III	×	✓	✓	✓	×	×	✓	×	-	×	✓	×
IV	-	✓	-	✓	×	✓	-	✓	-	-	-	×
V	×	×	×	-	-	-	-	×	✓	✓	✓	×
VI	×	✓	×	✓	×	×	×	×	×	✓	-	-
VII	×	✓	×	✓	✓	✓	✓	✓	×	✓	✓	✓
VIII	×	×	✓	×	×	×	×	×	×	×	✓	×

Table 1: Analysis Matrix

Trust and Reputation (I). As it was stated in Section 3.2, it is preferable to have different algorithms to compute trust and reputation. Trust is a richer concept that may take into account more information than the mere behaviour of the nodes.

Even though trust and reputation are different concepts they are used indistinctly sometimes. There are even some cases where reputation is completely ignored [37, 24, 20, 11, 30]. Some other approaches consider trust and reputation as different concepts and reputation is used as an input for computing trust values [7, 2, 19, 29, 27, 5].

In [19] the uncertainty of the monitoring process (i.e. the ignorance about the outcome of previous operations) is considered as an input for trust. In fact, the output of the Trust Module consists of three different values $< pt, nt, ut >$, where pt is the positive trust, nt is the negative trust and ut is the uncertainty in the decision of the Trust Module.

Base Station and Sensor Nodes (II). In order to broadcast control information and retrieve the readings from the sensors, the base station must be able to authenticate itself. Moreover, in most applications the base station acts as a permanent interface between the network and the users. Therefore, it can be inherently trusted. Still, none of the reviewed approaches use the base station as a trusted agent or as a helping entity for computing trust and/or reputation values. Only a few of them use it for solving conflicts or for notifying misbehaviours [37, 29]. The majority of the approaches do not even mentioned the BS [24, 20, 7, 2, 19, 11, 27, 25, 30, 5].

First-Hand Information Gathering (III). First hand information is considered most of the times but the way it is collected or, in other words, the sources of this information change from one approach to another. In general, first hand information encodes the behaviour of the neighbouring nodes. Most of the approaches deal with this behaviour as an abstract concept [7, 2, 11, 37, 5], however, some of them give an exact definition of it [27] or even consider different factors influencing the behaviour, such as routing, sensing or aggregation [24, 20, 19, 29, 30].

Second-Hand Information Gathering (IV). Using second hand information when computing trust is beneficial for several reasons [17]. One of them is the improvement on the convergence time as it could also help saving energy.

Whereas some recent approaches do not yet consider second hand information [7, 19, 5], those are an exception. Those that make use of second hand information can be separated in two groups depending on whether they provide some countermeasures to avoid dishonest recommendations or they do not. The approaches presented in [24, 19, 37, 27, 25, 30] do not provide or mention any functionality to protect the system from bad recommenders whereas [20, 2, 11, 29] do. Note that the existence of conflicting reports (as in the conflicting behaviour attack) is usually a clear indicative of an unknown problem in the network that should be notified. This particular fact is not considered in most proposals. Most of them use passive information gathering (i.e. requiring information only when it is needed). However, authors in [19] also consider a kind of push mechanism called *trigger method* where an agent can broadcast at any time any trust value which is below a predefined threshold.

Initial Values (V). At the beginning of the lifetime of a WSN all its nodes hold a good reputation and are equally trusted. This is not usually mentioned in most of the proposals [24, 11, 37, 29, 5] although some of them hold this property even without noticing it [20, 7, 2, 19]. Only a few proposals describe properly how and why initial values are considered [27, 25, 30].

Granurality (VI). Trust and reputation need a context to become relevant. Absolute trust is not practical. One node can be trusted for one task but not for another one. If the node sensing module is malfunctioning it does not mean that the node cannot be trusted for routing packets.

However, in most of the proposals [24, 7, 2, 19, 11, 37, 27] only one factor of trust and reputation is observed. Some proposals take into account the need for distinguishing different factors and nevertheless, when building trust, an absolute value is computed [30, 5].

In some other proposals multiple trust factors are observed and multiple trust/reputation values are computed [20, 29, 25]. In particular, [29] considers three independent parameters: routing, sensing and aggregation; with a different beta reputation distribution for each of them.

Updating and Aging (VII). Most of the solutions provide a smooth mechanism to update trust values during the life of the nodes, taking into account information about the context of the system [20, 7, 2, 19, 11, 29, 30, 5]. Some others do not address this issue [24, 37, 25, 27].

The proposal presented in [2] is of special relevance as the system is capable of managing mobile nodes. Whenever a node moves to a new neighbourhood, a monitor node that was in charge of storing its reputation can send its reputation to the new monitor node. Another proposal of special relevance is presented in [7], where a node that is marked as malicious loses its good reputation without any chance to recover it.

Risk and Importance (VIII). Most of the proposals do not take risk into account [20, 7, 2, 19, 11, 29, 5, 37, 25, 27]. Only a few of them deal with it [24, 30]. In particular, [24] introduces the concept of *Dispositional Trust* that is related to the amount of risk the node is ready to take in the absence of recommendations and experience.

4.2. Findings from the Analysis

By analyzing the results obtained in Section 4.1 (summarized in Table 1) we can observe that three of the *best practices* are not fulfilled by most of the proposals: *Trust and the Base Station* (II), *Granularity* (VI) and *Risk and Importance* (VIII). While it may be usual not to consider the use of a base station due to the decentralized nature of WSN, it is still a member of the network that can calculate certain trust values using its global position. Regarding risk and importance, they have not been widely considered in WSN applications although they may be interesting in the future as factors that can be used for assuring certain Quality of Service (QoS) in the communications. Moreover, although WSN applications are at present very simple (e.g. sense data and route information), the roles of the sensor nodes are not limited only to one task, therefore granularity should be taken into account.

Other *best practices* are considered by most trust management systems, although it should still be possible to modify the existing proposals or create new ones in order to offer a better compliance. For example, there are plenty of information sources for *First-Hand Information Gathering* (III) what could make the computed reputation and trust values be more precise if that wealth of information were to be fully considered. Besides, other important factors such as the *Initial Values* (V), should be fully considered by all the proposals due to their importance for the correct behaviour of the trust system.

Finally, no single trust management system fulfils all the principles introduced in this paper. This does not mean that they are not useful by themselves. Some proposals are constructed with a specific application in mind (e.g. clustering, routing) and can be used to protect that application.

Other proposals may not consider factors such as the use of the base station and sharing second-hand information, but their trust values can provide an interesting second opinion for the protocols of the WSN. Nevertheless, by trying to fulfil all the different *best practices*, a trust management system could be general enough to be applied to many different kinds of applications in different scenarios.

5. Conclusions and Future Work

Wireless Sensor Networks have been proven lately a very useful type of networks. As the development and research on this type of networks is still growing the need for including tools, such as trust or reputation is also growing. WSN will then turn our to be more useful for real worls applications. Thus, in this paper we have made an analysis of different approaches for Trust and Reputation management systems for Wireless Sensor Networks (WSN). Through this analysis we have identified a set of *Best Practices* that we consider are important and relevant. We believe these practices should be included in the design of a trust management system for WSN. According to the classification based on these best practices we have reviewed which existing approaches for trust or reputation systems for WSN take these practices into account. The success of the trust management system might depend on the adoption of the practices.

By analysing the existing approaches we have come to the conclusions that some of these practices are mostly overlooked by most of the proposals. This is the case, for example, of trust and reputation. In most of the cases they are considered jointly in order to build the trust or reputation systems. However, there are many other practices, such as *Trust and the Base Station*, *Risk and Importance* and *Granularity*, that are considered only by a few of the analyzed cases.

In the future we intend to build lightweight trust management systems for WSN that include or, at least consider as many of the best practices mentioned in this paper as possible. Besides, we will also analyze how the lack of a trust management system can affect the system. This will provide more accurate and reliable trust management systems for WSN.

Acknowledgements

This work has been funded by MEC I+D and MICT of Spain under the research projects CRISIS (TIN2006-09242), ARES (CSP2007-00004) and by

the European Commission through the research project SPIKE (FP7-ICT-2007-1-217098).

References

[1] T. Roosta A. Shah B. Sinopoli A. Giani, G. Karsai and J. Wiley. A Testbed for Secure and Robust SCADA Systems. *ACM SIGBED Review*, 5(2), 2008.

[2] F. Li A. Srinivasan and J. Wu. A Novel CDS-Based Reputation Monitoring System for Wireless Sensor Networks. In *28th International Conference on Distributed Computing Systems Workshops (ICDCS 2008)*, Beijing, China, June 2008.

[3] E. Aivaloglou, S. Gritzalis, and C. Skianis. Trust Establishment in Sensor Networks: Behaviour-based, Certificate-based and a Combinational Approach. *Int. J. System of Systems Engineering*, 1(1/2):128–148, 2008.

[4] Crossbow Solutions Blog. Radmote - Mobile Framework for Radiation Monitoring. `http://blog.xbow.com`. Accessed on October, 2009.

[5] A. Boukerch, L. Xu, and K. El-Khatib. Trust-based Security for Wireless Ad-Hoc and Sensor Networks. *Computer Communications*, 30:2413–2427, 2007.

[6] C. Chong and S. P. Kumar. Sensor Networks: Evolution, Opportunities, and Challenges. *Proceedings of the IEEE*, 91(8):1247–1256, 2003.

[7] G. V. Crosby and N. Pissinou. Cluster-based Reputation and Trust for Wireless Sensor Networks. In *4th IEEE Consumer Communications and Networking Conference (CCNC 2007)*, Las Vegas, USA, January 2007.

[8] G. V. Crosby, N. Pissinou, and J. Gadze. A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks. In *In Proceedings of the Second IEEE Workshop on Dependability in Sensor Networks and Systems (DSSNS'06)*. IEEE Computer Society, 2006.

[9] D. Estrin D. Culler and M. Srivastava. Overview of Sensor Networks. *IEEE Computer*, 37(8):41–49, 2004.

[10] D. Estrin D. Culler and M. Srivastava. Simplification and Analysis of Transitive Trust Networks. *Web Intelligence and Agent Systems*, 4(2):139–161, 2006.

[11] J. Zhiping D. Hongjun and D. Xiaona. An Entropy-based Trust Modeling and Evaluation for Wireless Sensor Networks. In *International Conference on Embedded Software and Systems (ICESS 2008)*, Chengdu, China, July 2008.

[12] T. Teixeira D. Jung and A. Savvide. Sensor Node Lifetime Analysis: Models and Tools. *ACM Transactions on Sensor Networks*, 5(1), 2009.

[13] S. Gritzalis E. Aivaloglou. TrustBased Data Disclosure in Sensor Networks. In *Communication and Information Systems Security Symposium (IEEE ICC 2009)*, Dresden, Germany, June 2009.

[14] C. Fernandez-Gago, R. Roman, and J. Lopez. A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks. In *3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007)*, IEEE, Istanbul (Turkey), July 2007.

[15] HART Communication Foundation. WirelessHART specification. `http://www.hartcomm.org/`. Accessed on October, 2009.

[16] J. Frey. Wisa Wireless Control in Theory, Practice and Production. Technical report, ABB, September 2008.

[17] S. Ganeriwal, L. Balzano, K. Srivastava, and B. Mani. Reputation-based Framework for High Integrity Sensor Networks. *ACM Trans. Sen. Netw.*, 4(3):1–37, 2004.

[18] S. Ganeriwal and M. B. Srivastava. Reputation-Based Framework for High Integrity Sensor Networks. In *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks.*, pages 66–77, Washington, DC, USA, 2004.

[19] J. Hu H. Chen, H. Wu and C. Gao. Agent-Based Trust Management Model for Wireless Sensor Networks. In *2nd International Conference on Multimedia and Ubiquitous Engineering (MUE 2008)*, Busan, Korea, April 2008.

[20] C. Deokjai H. Guangjie and L. Wontaek. A Reliable Approach of Establishing Trust for Wireless Sensor Networks. In *IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007)*, Dalian, China, September 2007.

[21] Y. Sankarasubramaniam I. Akyildiz, W. Su and E. Cayirci. Wireless Sensor Networks: A Survey. *Computer Networks*, 38(4):393–422, 3 2002.

[22] A. Jøsang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43:618–644, 2007.

[23] M. Krasniewski and B. Rabeler. TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks. In *DSN '05: Proceedings of the 2005 International Conference on Dependable Systems and Networks*, pages 672–681, Washington, DC, USA, 2005.

[24] G. P. Navarrete M. Momani, J. Agbinya and M. Akache. A New Algorithm of Trust Formation in Wireless Sensor Networks. In *1st IEEE International Conference on Wireless Broadband and Ultra Wideband Communciations (AusWireless'06)*, Sydney, Australia, March 2006.

[25] F. Gómez Mármol and G.Martínez Pérez. Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique. In *Proceedings of the Networking and Electronic Commerce Research Conference, NAEC'08*, Lake Garda, Italy, sep 2008.

[26] M. Mejia, N. Pea, J. L. Muoz, and O. Esparza. A Review of Trust Modeling in Ad Hoc Networks. *Internet Research*, 19:88–104, 2009.

[27] M. Momani, K. Aboura, and S. Challa. RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks. In *3rd International Conference on Intelligent Sensors, Sensor Networks and Information (ISSNIP 2007)*, pages 347–352, Dec. 2007.

[28] N. Foukia N. Lewis. Using Trust in Key Distribution in Wireless Sensor Networks. In *IEEE Workshop on Wireless Mesh and Sensor Networks (on GLOBECOM 2007)*, Washington, USA, November 2007.

[29] S. Ozdemir. Functional Reputation based Reliable Data Aggregation and Transmission for Wireless Sensor Networks. *Comput. Commun.*, 31(17):3941–3953, 2008.

[30] M. J. Probst and Sneha K. Kasera. Statistical Trust Establishment in Wireless Sensor Networks. In *ICPADS '07: Proceedings of the 13th International Conference on Parallel and Distributed Systems*, pages 1–8, Washington, DC, USA, 2007. IEEE Computer Society.

[31] R. Roman, M. C. Fernandez-Gago, J. Lopez, and H.-H. Chen. *On Security and Privacy in Mobile and Wireless Networking*, chapter Trust and Reputation Systems for Wireless Sensor Networks. Troubador Publishing Ltd, 2009.

[32] I. Woungang S. Misra and S.C. Misra, editors. *Guide to Wireless Sensor Networks*. Springer-Verlag/Heidelberg, 2009.

[33] R. A. Shaik, H. Jameel, S. Lee, S. Rajput, and Y. Jae Song. Trust Management Problem in Distributed Wireless Sensor Networks. In *12th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06)*, IEEE Computer Society, 2006.

[34] Y. Sun, Z. Han, and K.J.R Liu. Defense of Trust Management Vulnerabilities in Distributed Networks. *Communications Magazine, IEEE*, 46(2):112–119, February 2008.

[35] Crossbow Technology Inc. eKo Pro, Precision Agriculture. `http://www.xbow.com/eko/`. Accessed on October, 2009.

[36] W. Zhang, S. Das, and Y. Liu. A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks. In *Proceedings of the IEEE SECON 2006*, Reston, VA, September 2006.

[37] T. A. Zia. Reputation-based Trust Management in Wireless Sensor Networks. In *Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP 2008*, pages 163–166, December 2008.

[38] Z.Yao, D. Kim, I. Lee, K. Kim, and J. Jang. A Security Framework with Trust Management for Sensor Networks. In *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pages 190–198, 2005.